CentOS 防火墙设置

下边方式任选一种，建议第一种

防火墙开放 8080（Tomcat）、3306(Mysql)、27017(MongoDB)端口、8161(ActiveMQ Web 管理页)、61616(ActiveMQ BrokeUrl)

（1）可以进行下边操作：

如果要添加范围例外端口 如 1000-2000

语法命令如下：启用区域端口和协议组合

firewall-cmd [--zone=<zone>] --add-port=<port>[-<port>]/<protocol> [--timeout=<seconds>]

此举将启用端口和协议的组合。端口可以是一个单独的端口 <port> 或者是一个端口范围 <port>-<port> 。协议可以是 tcp 或 udp。

实际命令如下：

a. 添加

 # firewall-cmd --zone=public --add-port=8080/tcp --permanent #Tomcat

 # firewall-cmd --zone=public --add-port=3306/tcp --permanent #MySql

 # firewall-cmd --zone=public --add-port=27017/tcp --permanent #MongoDB

 # firewall-cmd --zone=public --add-port=8161/tcp --permanent #ActiveMQ Web 管理页

 # firewall-cmd --zone=public --add-port=61616/tcp --permanent # ActiveMQ BrokeUrl

说明：--permanent 永久生效，没有此参数重启后失效

firewall-cmd --zone=public --add-port=1000-2000/tcp --permanent

b. 重新载入

 # systemctl restart firewalld.service

c. 查看

 # firewall-cmd --zone=public --query-port=8080/tcp

 # firewall-cmd --zone=public --query-port=3306/tcp

 # firewall-cmd --zone=public --query-port=27017/tcp

 # firewall-cmd --zone=public --query-port=8161/tcp

 # firewall-cmd --zone=public --query-port=61616/tcp

c. 删除

firewall-cmd --zone= public --remove-port=80/tcp --permanent

（2）当然你可以还原传统的管理方式。

增加 8080、3306、27017 端口到防火墙配置中，执行以下操作：

vi /etc/sysconfig/iptables

增加以下代码

-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT

-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT

-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 27017 -j ACCEPT

service iptables start/stop

若报错 Failed to start iptables.service: Unit iptables.service failed to load: No such file or directory.

说明在 CentOS 7 或 RHEL 7 或 Fedora 中防火墙由 firewalld 来管理

a. 执行一下命令：

```
# systemctl stop firewalld
# systemctl mask firewalld
```

b. 安装 iptables-services：

```
# yum install iptables-services
```

c. 设置开机启动：

```
# systemctl enable iptables
# systemctl stop iptables
# systemctl start iptables
# systemctl restart iptables
# systemctl reload iptables
```

d. 保存设置：

```
# service iptables save
```

OK，再试一下应该就好使了

重启防火墙

```
# service iptables restart
```